J613-M0109-11 Rev.K 080521

Allied Telesis

CentreCOM 9408LC/SP・9424T/SP リリースノート

この度は、CentreCOM 9408LC/SP・9424T/SP をお買いあげいただき、誠にありがとうございました。
このリリースノートは、取扱説明書とコマンドリファレンスの補足や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。
最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1　ファームウェアバージョン　2.3.2J

2　本バージョンで修正された項目

ソフトウェアバージョン **2.3.1J** から **2.3.2J** へのバージョンアップにおいて、以下の項目が修正されました。

2.1 本製品に対して複数のクライアントから Telnet セッションの確立・切断を繰り返し行っているとき、SHOW FILE コマンド、CREATE CONFIG コマンドがエラーで実行できない場合がありましたが、これを修正しました。

2.2 本体宛ての Telnet など TCP 通信において、再送が発生した場合、メモリーが解放されませんでしたが、これを修正しました。

2.3 Telnet 経由でコマンドを実行中に Telnet セッションを強制切断すると、マネージメントの送受信バッファーが解放されないことがありましたが、これを修正しました。

2.4 Telnet 経由でコマンドを実行中にクライアントの接続ポートからケーブルを抜くと、マネージメントの送受信バッファーが解放されないことがありましたが、これを修正しました。

2.5 トランクグループからポートを削除した後、該当ポートに対して SET SWITCH PORT コマンドで複数のパラメーターを指定した設定を行うと、コンソールがハングアップすることがありましたが、これを修正しました。

2.6 CREATE QOS FLOWGROUP コマンドの PRIORITY パラメーターと、CREATE QOS POLICY コマンドの MOVEPRIORITYTOTOS パラメーターが同時に設定されていると、どちらの機能も正しく動作しませんでしたが、これを修正しました。

2.7 ポート認証と IGMP Snooping 併用時、IGMP パケットに対してポート認証が正しく動作しませんでしたが、これを修正しました。

2.8 MAC ベース認証の Authenticator ポートがリンクダウンすると、SNMP 用のメモリーが減少することがありましたが、これを修正しました。

2.9 本製品に HUB などを介して接続された端末を移動することで、本製品の接続ポートがリンクダウンをともなわずに変更された場合、ARP の登録が更新されず、本製品宛ての通信ができなくなっていましたが、これを修正しました。

2.10 ポート認証において、認証サーバーリストから削除された RADIUS サーバー宛てに Access-Request パケットが送信されていましたが、これを修正しました。

2.11 本製品の Authenticator ポートから EAP-Request（MD5）が再送信される場合のパケットフォーマットが正しくありませんでしたが、これを修正しました。

2.12 SET PORTAUTH PORT ま た は、SET PORTACCESS PORT コ マ ン ド の QUIETPERIOD パラメーターにハイフン（-）が指定できていましたが、これをできないように修正しました。

2.13 SHOW CONFIG コマンドの DYNAMIC パラメーターに PORTAUTH を指定できませんでしたが、これを修正しました。

2.14 ダイナミック VLAN によって Authenticator ポートの所属 VLAN を動的にアサインしようとしたとき、該当の Authenticator ポートに隣接するポートがタグ付きポートとして所属している VLAN をアサインさせようとすると、認証に失敗していましたが、これを修正しました。

2.15 IP ヘッダーの終点 IP アドレスに IP マルチキャストアドレス、IP ペイロードに TCP ヘッダーを持った本製品 MAC アドレス宛てのパケットを受信すると、本製品がクラッシュしていましたが、これを修正しました。

2.16 大量の ARP Request を受信し続けている状態で、本製品を起動すると起動後に ARP 解決ができない場合がありましたが、これを修正しました。

3 本バージョンでの制限事項

ファームウェアバージョン **2.3.2J** には、以下の制限事項があります。

3.1 攻撃検出

参照 **「コマンドリファレンス」/「運用・管理」/「攻撃検出」**

ファームウェアバージョン 2.3.1J リリースノートに掲載いたしました「4.7 攻撃検出」ですが、その後の調査によって、9408LC/SP および 9424T/SP では発生しないことが判明したため、制限事項から削除しました。

3.2 クラシファイア

参照 **「コマンドリファレンス」/「クラシファイア」**

ファームウェアバージョン 2.3.1J リリースノートに掲載いたしました「4.17 クラシファイア」ですが、その後の調査によって、9408LC/SP および 9424T/SP では発生しないことが判明したため、制限事項から削除しました。

3.3 IP インターフェース

参照 **「コマンドリファレンス」/「IP」/「IP インターフェース」**

ファームウェアバージョン 2.3.1J リリースノートに掲載いたしました「4.22 IP インターフェース」ですが、その後の調査によって、9408LC/SP および 9424T/SP では発生しないことが判明したため、制限事項から削除しました。

3.4 ポート認証と攻撃検出機能の併用

ポート認証と攻撃検出機能は併用できません。

3.5 802.1X 認証とスパニングツリーの併用

802.1X 認証とスパニングツリーは併用できません。

3.6 IGMP Snooping とポートセキュリティーの併用

IGMP Snooping とポートセキュリティーは併用できません。

3.7 ポートトランキングと Multiple STP の併用

ポートトランキングと Multiple STP は併用できません。

3.8 光ファイバーケーブル

光ファイバーケーブルを抜き差しする場合は、必ず、RX、TX 両方のケーブルを抜き差ししてください。RX 側のケーブルのみ抜き差しすると、通信が復旧しない場合があります。

3.9　コンパクトフラッシュ

参照 「コマンドリファレンス」/「運用・管理」/「記憶装置とファイルシステム」

コンパクトフラッシュのファイルに対して、ディレクトリーを指定して以下のコマンドを実行することができません。

- COPY
- RENAME
- DELETE
- SET CFLASH DIR

3.10 TFTP サーバーを使用したアップロード・ダウンロード

参照 「コマンドリファレンス」/「運用・管理」/「アップロード・ダウンロード」

TFTP サーバーからダウンロードした 45Byte より小さいファイルを TFTP サーバーにアップロードすると、本製品がリブートすることがあります。

3.11 ログ

参照 「コマンドリファレンス」/「運用・管理」/「ログ」

○　ログ機能が Disabled（無効）の状態で PURGE LOG コマンドを実行するとログ機能が Enabled（有効）になります。

○　SAVE LOG コマンドで保存されたログファイルを、SHOW FILE コマンドで表示させると、最後の行にエラーメッセージが表示されます。

3.12 SNMP

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

複数の SNMP マネージャーから同時にプライベート MIB の取得を繰り返し行っていると、本製品の SNMP エージェントが応答しなくなる場合があります。

3.13 ポートトランキング

参照 「コマンドリファレンス」/「スイッチ」/「ポート」

CREATE SWITCH TRUNK コマンドの SELECT パラメーターに MAC アドレスの選択基準（MACSRC、MACDEST、MACBOTH）が指定されていると、ルーティング後のパケットが負荷分散されずに送出されます。

3.14 バーチャル LAN

参照 「コマンドリファレンス」/「バーチャル LAN」

○　Protected Ports VLAN のクライアントポートとタグ付きポートは同一ポートに設定できない仕様ですが、先にクライアントポートを設定し、同一ポートをタグ付きポートにする設定を行うと、設定がエラーではじかれません。

○　SET SWITCH MULTICASTMODE コマンドで B（BPDU/EAP パケットを、VLAN を超えて、すべてのポートに転送する）が設定されていると、マルチプル VLAN（Protected Ports VLAN）のグループを超えて BPDU/EAP パケットが同一 VLAN 内にフラッディングされます。

○ ゲスト VLAN を設定している VLAN に、DESTROY VLAN コマンドを実行すると、VLAN が削除されてしまいます。

3.15 スパニングツリー

参照 「コマンドリファレンス」/「スパニングツリープロトコル」/「STP」

スパニングツリー有効時、DISABLE SWITCH PORT コマンドを実行すると、SHOW STP PORT コマンドの表示項目「State」において、該当ポートが Blocking で表示されます。表示上の問題であり、動作には問題ありません。

3.16 ラピッドスパニングツリー

参照 「コマンドリファレンス」/「スパニングツリープロトコル」/「Rapid STP」

○ Rapid STP 有効時、DISABLE SWITCH PORT コマンドを実行すると、SHOW RSTP コマンドに PORTSTATE パラメーターを指定して表示される「Enable」において、該当ポートが Disabled で表示されます。表示上の問題であり、動作には問題ありません。

○ Rapid STP 有効時、トポロジーチェンジ発生時にエッジポートに設定されたポートの FDB が消去されます。

3.17 ポリシーベース QoS

参照 「コマンドリファレンス」/「QoS」/「ポリシーベース QoS」

○ トラフィックが同一 QoS ポリシー内の複数のトラフィッククラスにマッチした場合、CREATE QOS TRAFFICCLASS コマンドの MAXBANDWIDTH パラメーター（最大帯域設定）が正しく動作しません。
MAXBANDWIDTH パラメーターを指定する場合は、同一 QoS ポリシー内で、複数のトラフィッククラスにマッチするような設定（IP と TCP、TCP と TCP ポートなど一方がもう一方を包括するようなフィルターの指定）をしないようにしてください。

○ CREATE QOS POLICY コマンドの REDIRECTPORT パラメーターでトラフィックの出力先ポートとして指定されたポートから送出されるパケットにタグが付与されます。ただし、9424T/SP の場合、REDIRECTPORT に指定されたポートと同じポートグループ（1 ～ 12 のグループまたは 13 ～ 24 のグループ）内から転送されたパケットに限り、本現象が発生します。

○ SET QOS TRAFFICCLASS コマンドの EXCEEDREMARKVALUE パラメーターに NONE を指定することができません（エラーではじかれます）。EXCEEDREMARKVALUE パラメーターを NONE に戻す場合は、該当のトラフィッククラスを DESTROY QOS TRAFFICCLASS コマンドで一度削除し、トラフィッククラスを作成しなおしてください。

3.18 QoS

参照 「コマンドリファレンス」/「QoS」/「QoS」

SET QOS SCHEDULING コマンドに WRR（ラウンドロビン）、WEIGHTS パラメーターの Q7 に 0（ゼロ）を指定して、キュー 7 が最優先（STRICT）になる設定をした場合、ユーザープライオリティー値 7 を持つフラッディングパケットが最優先で転送されません。

3.19 ハードウェアパケットフィルター

参照 「コマンドリファレンス」/「ハードウェアパケットフィルター」

○ ハードウェアパケットフィルターではアクションに許可（permit）が指定されているエントリーが最優先で処理される仕様ですが、エントリーが複数作成されていると、エントリー番号の大きいエントリーが優先的に処理される場合があります。エントリーを複数作成する場合は、アクションに許可（permit）が指定されているエントリーが最後（最も大きい番号）になるように設定してください。

○ ハードウェアパケットフィルターでアクションに許可（permit）を指定したエントリーに、アクションを破棄（deny）に指定したエントリーよりも大きなエントリー番号を設定しても、許可（permit）を指定したエントリーが正しく処理されない場合があります。

3.20 ポート認証

参照 「コマンドリファレンス」/「スイッチング」/「ポート認証」

○ ポートを Authenticator ポートに設定すると、同ポートで自動的にイーグレスフィルタリングが有効になり、その設定が設定ファイルに書き込まれます。Authenticator ポートではイーグレスフィルタリングが有効になっている必要がありますので、イーグレスフィルタリングの設定は変更しないようにしてください。

○ ポート認証で Single-Supplicant モードの場合、EAP-Request パケットの宛先は、条件により異なります。
サプリカント対象の MAC アドレスを FDB に学習していない場合は、マルチキャストで送信しますが、学習後は、ユニキャストで送信します。

○ ポートを 802.1X Authenticator ポートに設定すると、設定ファイルにイーグレスフィルタリングを有効にする設定が自動的に書き込まれますが、802.1X 認証を無効にしても、イーグレスフィルタリング有効の設定が解除されません。

○ ポートを 802.1X Authenticator ポートに設定すると、設定ファイルに「set switch port=xx securitymode=pacontrol」という設定（未サポートのセキュリティーモード設定）が自動的に書き込まれます。

○ SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの SERVERTIMEOUT/SERVTIMEOUT パラメーターに 31（秒）以上の値を指定すると、タイムアウト値が 60（秒）で動作します。

○ ポートがリンクダウンしているときに、SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの CONTROL パラメーターを設定変更できません。

○ SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの MODE パラメーターに MULTI、CONTROL パラメーターに AUTHORISED を指定しているとき、SHOW PORTAUTH（PORT）または SHOW PORTACCESS（PORT）コマンドでサプリカント数が正しく表示されない場合があります。

○ 802.1X Authenticator ポートまたは MAC ベース認証ポートに、ADD SWITCH FILTER コマンドによるスタティック MAC アドレスの登録が可能です。登録されたスタティッ

ク MAC アドレスで通信することはできません。

○　ダイナミック VLAN で、認証されたポートを別の MST インスタンスに所属する VLAN に指定した場合、同一 VLAN 内でも通信ができなくなります。

○　MAC ベース認証時、本製品の Authenticator ポートに HUB などを介して接続されているサプリカントを一度 HUB からはずし、再接続すると認証ができません。

○　ポートに対して、最初に Supplicant/Authenticator ポートの設定を行い、次に VLAN の設定（タグなしポートとして設定）を行うと、エラーで VLAN の設定ができません。また、本製品の仕様では、Supplicant/Authenticator ポートをタグ付きに設定することはできませんが、上記手順でタグ付きの設定を行っても、エラーにはなりません。
Supplicant/Authenticator ポートの設定を行う場合は、最初に VLAN の設定を行うようにしてください。

○　MAC ベース認証では、サプリカントの MAC アドレスがエージングにより FDB から削除されると、認証許可状態が解除されます。

○　ポートがゲスト VLAN に割り当てられているとき、ゲスト VLAN に所属する別の PC から未学習のユニキャストアドレスでは通信できません。

○　Authenticator ポートにゲスト VLAN を設定している状態で、DISABLE PORTAUTH コマンドを実行しても、ゲスト VLAN に割り当てられてしまいます。

3.21 ARP

参照 「コマンドリファレンス」/「IP」/「ARP」

異なるネットワークから本製品（CPU）宛ての通信を連続的に行うと、ARP が解決しているにもかかわらず、ARP Request が送信される場合があります。

3.22 IPv6 マルチキャスト

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」

○　IPv6 マルチキャストと一致した MAC アドレスのパケットを受信すると、マルチキャストグループとして登録してしまうことがあります。

○　マルチキャストルーターに接続されるポートが存在しない状態で、Multicast Listener Report を受信すると、すべてのポートに転送されます。

4 取扱説明書・コマンドリファレンスの補足・誤記訂正

同梱の取扱説明書「CentreCOM 9424T/SP・9408LC/SP 取扱説明書（J613-M0109-10 Rev.C）」、および「CentreCOM 9424T/SP・9408LC/SP コマンドリファレンス 2.3（J613-M0109-12 Rev.F）」の補足事項です。

4.1 エンハンストスタッキング

参照 「コマンドリファレンス」/「運用・管理」/「エンハンストスタッキング」

ファームウェアバージョン 2.3.1J リリースノートに掲載いたしました「5.1 エンハンストスタッキング」ですが、その後の調査によって、9408LC/SP および 9424T/SP では発生しないことが判明したため、下記の項目をコマンドリファレンスの補足から削除しました。

SNMPv3 を使用して、エンハンストスタッキンググループのスレーブスイッチにアクセスすることはできません。

4.2 フォワーディングデータベース

参照 「コマンドリファレンス」/「フォワーディングデータベース」

ファームウェアバージョン 2.3.1J リリースノートに掲載いたしました「5.6 フォワーディングデータベース」ですが、その後の調査によって、9408LC/SP および 9424T/SP では発生しないことが判明したため、下記の項目をコマンドリファレンスの補足から削除しました。

IP インターフェースを複数作成すると、FDB に PORT0（ゼロ）の MAC アドレス（本製品の MAC アドレス）が複数表示されます

4.3 エンハンストスタッキング

参照 「コマンドリファレンス」/「運用・管理」/「エンハンストスタッキング」

○ マスタースイッチからスレーブスイッチに SNMP 経由でエンハンストスタッキング接続している最中に、他のスイッチから該当のマスタースイッチに Telnet や SNMP による接続を行わないでください。

○ エンハンストスタッキングを使用する場合、マスタースイッチとスレーブスイッチを接続するには、下記のとおりに接続してください。

- スレーブスイッチ側は、Default_VLAN に所属するポートにマスタースイッチを接続してください。Default_VLAN 以外の VLAN に所属するポートに接続した場合は、IP インターフェースを作成して IP アドレスを設定しなければなりません。
- マスタースイッチ側は、ローカルインターフェースに設定した VLAN に所属するポートにスレーブスイッチを接続してください。

4.4 本製品起動時のご注意

本製品の電源をオンにしてから起動が完了するまでの間は、電源ケーブルを抜いたり、リセットボタンを押したりしないでください。

4.5 認証サーバー

参照 「コマンドリファレンス」/「運用・管理」/「認証サーバー」

ADD RADIUSSERVER コマンドで認証サーバーリストに追加された RADIUS サーバーと本製品が接続された状態で、ENABLE AUTHENTICATION コマンドにより認証が有効の場合は、RADIUS サーバーに登録したログイン名 / パスワードでしか本製品にログインすることができません。
本製品に設定されているユーザー名 / パスワードでログインする場合は、ENABLE AUTHENTICATION コマンドを実行しないでください。

4.6 SNMP

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

○ プライベート MIB の atiStkSwSysProductInfo Table 内の atiStkSwSysDCState が正しい値を返しません。リダンダント電源装置「CentreCOM RPS3204」使用時は、SHOW SYSTEM コマンドで本製品の電源とリダンダント電源装置の電源の On/Off を確認してください。

○ ブリッジ MIB の dot1dStpPort Table 内の dot1dStpPortEnable を変更しても設定は変更されません。本製品では、ポート単位でスパニングツリープロトコルの有効 / 無効を変更することができません。

○ SNMP マネージャーからシステム名を設定した場合、ログアウト / ログイン後にシステム名がプロンプトに反映されます。

4.7 SNMP コミュニティー名の使用可能文字種

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

SNMP コミュニティー名には、半角英数字だけでなく、半角記号も使用できるようになりました。ただし、「[（スクエアブラケット）」「"（ダブルクォーテーション）」「¥（バックスラッシュ（円マーク））」「（半角スペース）」は使用できません。

4.8 フォワーディングデータベース

参照 「コマンドリファレンス」/「フォワーディングデータベース」

○ リンクダウンをともなわない端末移動があった場合、学習機能により登録された MAC アドレスがエージングするまで、通信が復旧しないことがあります。

○ ポートグループ 1 ～ 12 とポートグループ 13 ～ 24 グループ間で通信を行った場合、同一の MAC アドレスがどちらのポートの FDB にも表示される場合があります。

○ 予約マルチキャストアドレスを、FDB にスタティックエントリーとして登録することはできません。

4.9 複数ポートから 1 ポートへの通信

参照 「コマンドリファレンス」/「スイッチング」

○ Jumbo フレームを複数ポートから 1 ポートに対して同時に送信すると、受信した 1 ポートからフレームが転送されません。

○ ポートグループ 1 ～ 12 とポートグループ 13 ～ 24 グループ間の通信において、複数ポートから 1 ポートに対して同時にパケットを送信し、パケットロスが発生した場合、送信ポートによってパケットの損失率にばらつきがあります。

4.10 ポートトランキング

参照 「コマンドリファレンス」/「スイッチング」/「ポートトランキング」

トランキンググループの最若番ポートを抜き差しすると、接続の組み合わせによって、ポートのリンクアップトラップが生成されない場合があります。

4.11 ポートミラーリング

参照 「コマンドリファレンス」/「スイッチング」/「ポートミラーリング」

ポートミラーリング機能が有効の場合、「01:80:C2:00:00:00」などの予約マルチキャストアドレスをソースポートで受信すると、ミラーポートからパケットが重複して送信されます。

4.12 バーチャル LAN

参照 「コマンドリファレンス」/「バーチャル LAN」

DELETE VLAN コマンドを使用し、ポートを VLAN から削除するコマンドの記載に誤りがありましたので、訂正してお詫びいたします。

誤：DELETE VLAN=default PORT=4
正：DELETE VLAN=default_VLAN PORT=4

4.13 ポリシーベース QoS

参照 「コマンドリファレンス」/「QoS」/「ポリシーベース QoS」

○ CREATE QOS TRAFFICCLASS コマンドの MAXBANDWIDTH パラメーターに 0（ゼロ）を指定すると、帯域ゼロのトラフィッククラスが作成されますが、このトラフィッククラスが割り当てられた QoS ポリシー作成直後の一定量の通信、および本製品再起動直後の一定量の通信に限り、該当ポートからのトラフィックがフィルターされません（帯域ゼロになりません）。

○ 出力ポートに QoS ポリシーを関連づけた場合、フィルター対象となるのは学習済みのユニキャストアドレス宛てのトラフィックのみです。未学習のユニキャスト / マルチキャストアドレス、およびブロードキャスト宛てのトラフィックは対象になりません。また、学習済みのマルチキャストアドレス宛てのトラフィックも対象になりません。

4.14 ポート認証

参照 「コマンドリファレンス」/「スイッチング」/「ポート認証」

○ ポート認証有効時、RADIUS サーバーを 3 台登録し、本製品からの Access-Request に対して 3 台とも応答がないと、全サーバーに対して同時に Access-Request パケットが再送信されます。

○ ポート認証有効時、RADIUS サーバーを 3 台登録し、優先順位 3 のサーバーでのみ認証が行われた場合、認証のたびに 3 台のサーバーに対して Access-Request パケットが送信されます。
また、優先順位 2 のサーバーでのみ認証が行われた場合は、優先順位 1 と 2 のサーバー

に対して Access-Request パケットが送信されます。

○ SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの TYPE/ROLE パラメーターに NONE を指定すると、指定ポートの設定をデフォルトに戻すことができますが､このとき､PORTAUTH/PORTACCESS パラメーターに認証メカニズム（802.1X または MACBASED）を指定する必要はありません。MAC ベース認証の設定であっても、MACBASED の指定をせずにコマンドを入力してください（指定するとエラーになりコマンドが実行されません）。

○ SET PORTAUTH PORT または SET PORTACCESS PORT コマンドで PORTAUTH/PORTACCESS パラメーターに MACBASED を指定した際、使用できるパラメーターの記載に誤りがありましたので、訂正してお詫びいたします。
MODE={MULTI¦SINGLE} パラメーターも指定可能です。

4.15 バーチャル LAN

参照 「コマンドリファレンス」/「バーチャル LAN」

MAC アドレス VLAN に MAC アドレスを追加したとき、別の VLAN から、MAC アドレス VLAN に追加した MAC アドレスを送信元 MAC アドレスとして持つ機器同士で双方向のユニキャスト通信を行うと、パケットが転送されてしまいます。

4.16 マルチプル VLAN（Protected Ports VLAN）

参照 「コマンドリファレンス」/「バーチャル LAN」

複数の Protected Ports VLAN が存在し（例えば VLAN10 と VLAN20 が存在するような場合）、アップリンクポートの一部を共有している場合、VLAN10 のクライアントから VLAN20 宛てにパケットを送信すると、VLAN20 のアップリンクポートだけでなくクライアントポートにも送信されます。

4.17 ラピッドスパニングツリー

参照 「コマンドリファレンス」/「スパニングツリープロトコル」/「Rapid STP」

○ ラピッドスパニングツリープロトコルを有効にし、トランクグループに所属したポートがリンクアップすると、そのポートの通信速度の設定に関係なく、ポートプライオリティーが 64、パスコストが 2000 に設定されます。

○ ACTIVATE STP/MSTP コマンドを実行すると、設定ファイルに保存されますが、ACTIVATE RSTP コマンドを実行しても、設定ファイルには保存されません。

4.18 MLD Snooping

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

マルチキャストルーターが接続されるポートが存在しない状態で、Multicast Listener Report を受信すると、すべてのポートに転送されます。
SET IPV6 MLDSNOOPING コマンドの ROUTERPORT パラメーターでポートを設定すれば転送されません。

5　未サポートコマンド（機能）

以下のコマンド（パラメーター）はサポート対象外ですので、あらかじめご了承ください。

SET SYSTEM DISTINGUISHEDNAME
MENU
SET SWITCH CONSOLEMODE
SET AUTHENTICATION METHOD=TACACS
ADD/DELETE TACACS SERVER
SET SWITCH PORT
[BACKPRESSURE={YES¦NO¦ON¦OFF¦TRUE¦FALSE¦ENABLED¦DISABLED}]
[BPLIMIT={1..7935}][FCTRLLIMIT={1..7935}]
SET SWITCH PORT SECURITYMODE=PACONTROL
CREATE/DESTROY/ADD/DELETE/SET/SHOW LACP
ENABLE/DISABLE/SET/SHOW PURGE GARP
SET VLAN={vlanname¦1..4049}[TYPE=PORTBASED]
CREATE/ADD/DELETE/SET/SHOW/PURGE PKI
SET/SHOW SSL

6　取扱説明書／コマンドリファレンスについて

最新の取扱説明書「CentreCOM 9424T/SP、9408LC/SP 取扱説明書（J613-M0109-10 Rev.C）」およびコマンドリファレンス「CentreCOM 9424T/SP、9408LC/SP コマンドリファレンス 2.3（J613-M0109-12 Rev.F）」は弊社ホームページに掲載されています。
本リリースノートは、上記のマニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社 Web ページで最新の情報をご覧ください。

※取扱説明書のパーツナンバー「J613-M0109-10 Rev.C」は 1 ページ目（表紙）に、コマンドリファレンスのパーツナンバー「J613-M0109-12 Rev.F」は、コマンドリファレンスの全ページ（左下）に入っています。

http://www.allied-telesis.co.jp/